

# OPTICAL ORTHOGONAL CODES USING QUADRATIC RESIDUES

Manoj Choudhary\*

Samsung India Software Operations  
No. 67, Infantry Road  
Bangalore - 560001  
manojc@samsung.com

P. K. Chatterjee

Dept. of Electrical Engg.  
IIT Kanpur  
India - 208016  
pralayk@iitk.ac.in

Joseph John

Dept. of Electrical Engg.  
IIT Kanpur  
India - 208016  
jjohn@iitk.ac.in

## ABSTRACT

The positivity of the optical correlators render the extensively studied bipolar spreading codes unsuitable for all optical networks such as Fiber Optic CDMA systems, thereby motivating the study of truly positive code sequences. Several such codes, constructed using Prime Sequences, Quadratic Congruences, Projective Geometry, Error correcting codes etc., have been studied earlier in the literature. This paper presents a method of constructing such Optical Orthogonal Codes (OOCs) using Quadratic Residues. These OOCs are of the form  $(p^2, p, 2, 2)$ , where  $p$  is a prime. We see that these codes have better crosscorrelation properties than OOCs based on Quadratic Congruences.

## 1. INTRODUCTION

The requirement of a very large bandwidth limits the use of CDMA in systems where the bandwidth is not at a premium. Optical fiber is such a medium where virtually unlimited bandwidth is available, and high capacity systems can be implemented using the CDMA technique. However, a substantial propagation delay compared to transmission time makes CDMA more suitable to Fiber Optic Local Area Networks (LANs). The fact that CDMA supports asynchronous transmissions, is particularly helpful when the transmissions are asynchronous, random and bursty as in the case of LANs.

The advantages of fiber optics and rapid developments in optical signal processing are leading towards

---

Previously with Department of Electrical Engineering, Indian Institute of Technology, Kanpur.

all optical networks. The use of CDMA in fiber optic LANs has been proposed by Salehi et. al. in [1, 2]. The fiber optic CDMA takes advantage of excess bandwidth in single mode fibers to map low information rate electrical or optical signals into high rate optical pulse sequences to achieve multiple access communications, with little network control amongst the users. A typical link in a FO-CDMA communication system is shown in Fig. 1.

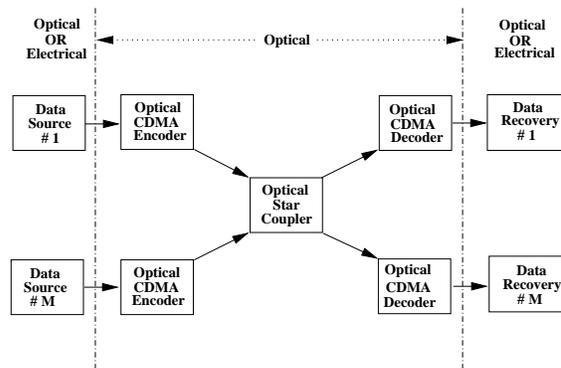


Figure 1: A FO-CDMA system in star configuration with  $M$  users.

In order to extract data from the desired optical pulse sequence at the receiver in the presence of all other users' pulse sequences, we require code sequences that satisfy two conditions[1], namely:

- 1) each sequence should be easily distinguishable from a shifted version of itself, and
- 2) each sequence should be easily distinguishable from (a possibly shifted version of) every other sequence in the set.

The above two conditions imply that the autocorrelation of any code sequence (except for zero shift) should be small, and the maximum crosscorrelation between any two code sequences should be zero. However, (0,1) sequences for truly positive systems, such as optical systems, can not achieve a crosscorrelation value of 0, as the coincidences do not cancel out unlike in (-1,+1) sequences. Hence, the minimum possible value of crosscorrelation is 1. Such codes are referred to as Optical Orthogonal Codes<sup>1</sup>.

An Optical Orthogonal Code is represented in the form of  $(n, w, \lambda_a, \lambda_c)$ , where  $n$  is the length of code sequence in the code, weight of each code sequence is  $w$ ,  $\lambda_a$  is the maximum off-peak autocorrelation, and  $\lambda_c$  denotes the maximum crosscorrelation value between any two codewords. It is desirable to have OOCs with the largest possible number of codewords, given the parameters  $n, w, \lambda_a$  and  $\lambda_c$ .

Some of the Optical Orthogonal Codes proposed in the literature include those using Prime Sequences[3], Quadratic Congruences[4], and Projective Geometry[5] etc. These codes have been discussed and a brief comparison presented in [6]. Some new classes of OOCs constructed using well known Hadamard Matrices[7], Error Correcting Codes[8], Skolem Sequences, Number Theory etc. have been discussed in [9].

In the next section, we introduce various parameters and notations used in the Optical Orthogonal Codes (OOCs). In section 3, we discuss the construction of Optical Orthogonal Codes using Quadratic Residues. We include an example for illustrating the procedure. We conclude the paper in section 4.

## 2. OPTICAL ORTHOGONAL CODES

An  $(n, w, \lambda_a, \lambda_c)$  Optical Orthogonal Code  $C$  is a family of (0,1) sequences of length  $n$  and weight  $w$  that satisfy the following bound on the maximum off-peak

---

<sup>1</sup>Since maximum crosscorrelations cannot be 0 in case of (0,1) codes, optical codes with small values of crosscorrelation are referred to as Optical Orthogonal Codes (OOCs) in the literature.

autocorrelation  $\lambda_a$ :

$$\sum_{t=0}^{n-1} x_t x_{t+\tau} \leq \lambda_a, \quad (1)$$

for any code sequence (also referred as codeword)  $X = \{x_0, x_1, \dots, x_{n-1}\} \in C$  and any integer shift  $\tau$  such that,  $0 < \tau < n$ . The maximum crosscorrelation  $\lambda_c$  satisfy the following bound:

$$\sum_{t=0}^{n-1} x_t y_{t+\tau} \leq \lambda_c, \quad (2)$$

for any two code sequences  $X, Y$  such that  $X \neq Y \in C$  and any integer shift  $\tau$  such that,  $0 \leq \tau < n$ .

Since each code sequence of  $C$  has a Hamming weight  $w$ , therefore, the autocorrelation peak for any code sequence is  $w$ . This happens for zero delay (i.e.,  $\tau = 0$ ). A codeword of length  $n$  has chip positions from 0 to  $(n - 1)$ .

An Optical Orthogonal Code  $C$  can also be considered as a family of  $w$ -sets of integers modulo  $n$ , in which each  $w$ -set corresponds to a codeword, and the integers within each  $w$ -set specify the nonzero bit positions of the codeword. Then the correlation properties can be reformulated as given below:

1) the autocorrelation property:

$$|(a + X) \cap (b + X)| \leq \lambda_a, \quad (3)$$

for any  $X \in C$  and any  $a \not\equiv b \pmod{n}$ , and

2) the crosscorrelation property:

$$|(a + X) \cap (b + Y)| \leq \lambda_c, \quad (4)$$

for any  $X \neq Y \in C$  and any  $a, b$ .

Here  $a + X = \{a + x : x \in X\}$  and all integers under consideration are taken modulo  $n$ . The set theoretic notion offers a convenient notation for OOCs when  $w$  is much smaller than  $n$ . In the set theoretic perspective, autocorrelation and the crosscorrelation properties can also be interpreted as follows:

1) autocorrelation: for any  $X \in C$ , any integer  $c \neq 0$  can be represented as the difference  $x - x'$ , with  $x, x' \in$

$X$ , in at most  $\lambda_a$  ways, and

2) crosscorrelation: for every pair of  $w$ -sets  $X \neq Y \in C$ , any integer  $c \neq 0$  can be represented as the difference  $x - y$ , with  $x \in X, y \in Y$ , in at most  $\lambda_c$  ways.

The size of a code  $C$ , denoted by  $M$ , is the number of codewords in it. The cyclic shift of a codeword is not considered as another codeword. It is desirable to have OOCs with the largest possible number of codewords  $M$ , given the parameters  $n, w, \lambda_a$  and  $\lambda_c$ . A good optical orthogonal code has many more 0's than 1's in each code sequence as that reduces the number of coincidences. Optical codes approach orthogonality (achieve quasi-orthogonality) by minimizing coincidences rather than by cancellation.

### 3. OOCs USING QUADRATIC RESIDUES

In this section, we present the construction of Optical Orthogonal Codes using Quadratic Residues. These codes are variants of OOCs obtained using Quadratic Congruences[4]. As described in [4], the OOCs using Quadratic Congruences are of the form  $(p^2, p, 2, 4)$ , where  $p$  is a prime, meaning that the maximum value of peak crosscorrelation  $\lambda_c$  is 4 which is quite high, and may deteriorate the multiple user performance. The OOCs presented in this paper have the value of  $\lambda_c$  equal to 2, while keeping all other code parameters exactly the same as in [4].

For any prime  $p$ ,  $a$  is a *Quadratic Residue* mod  $p$  if  $x^2 \equiv a \pmod{p}$  for any integer  $x$ . For any prime  $p$ , there are as many quadratic residues (QR) as there are quadratic non-residues. For example, when  $p = 11$ , the QRs are  $\{0, 1, 3, 4, 5, 9\}$ .

#### 3.1. Construction of Codes

Optical Orthogonal Codes can be constructed using Quadratic Residues (QR) using the following steps:

1. For any prime  $p$ , let the quadratic residues be  $X = \{0, x_1, x_2, \dots, x_{(p-1)/2}\}$ . There is a total of  $(p-1)/2$  quadratic residues. 0 is a quadratic residue (QR) as well as a quadratic non-residue.

2. Write the QR sequence as  $QR = \{q_1, q_2, \dots, q_p\}$ , where  $q_1 = q_p = 0, q_2 = x_1, q_3 = x_2$  and so on, and  $q_k = q_{p-k+1}$  for  $1 \leq k \leq p$ . This forms the first QR sequence, denoted by  $Q_1$ .

3. The  $j^{th}$  QR sequence,  $j \in \{1, 2, \dots, p-1\}$ , can be generated using  $Q_1$  by multiplying each element of  $Q_1$  by  $j$  (modulo  $p$ ).

4. Translate these QR sequences into  $(p-1)$  codewords by time-mapping the bit positions.

#### Example 3.1: OOCs USING QUADRATIC RESIDUES

Let us take a prime number,  $p = 5$ . The QRs for this are  $\{0, 1, 4\}$ . The number of QR sequences is equal to,  $p-1 = 4$ . The first QR sequence,  $Q_1$ , is  $\{0, 1, 4, 1, 0\}$ . The remaining QR sequences,  $Q_2, Q_3$  and  $Q_4$ , obtained using Step 3, are:

$$\begin{aligned} Q_2 &= \{0, 2, 3, 2, 0\} \\ Q_3 &= \{0, 3, 2, 3, 0\} \\ Q_4 &= \{0, 4, 1, 4, 0\} \end{aligned}$$

The corresponding codewords are:

$$\begin{aligned} C_1 &= \{10000 \ 01000 \ 00001 \ 01000 \ 10000\} \\ C_2 &= \{10000 \ 00100 \ 00010 \ 00100 \ 10000\} \\ C_3 &= \{10000 \ 00010 \ 00100 \ 00010 \ 10000\} \\ C_4 &= \{10000 \ 00001 \ 01000 \ 00001 \ 10000\} \end{aligned}$$

The length of each of these codewords is 25. In terms of  $w$ -sets, these codewords can be represented (modulo 25) as shown below.

$$\begin{aligned} C_1 &= \{0, 6, 14, 16, 20\} \\ C_2 &= \{0, 7, 13, 17, 20\} \\ C_3 &= \{0, 8, 12, 18, 20\} \\ C_4 &= \{0, 9, 11, 19, 20\} \end{aligned}$$

The autocorrelation of codewords  $C_1$  and  $C_3$  of example 3.1 is shown in Fig. 2 and Fig. 3, respectively. As can be seen from Figs. 2 and 3, the peak value of autocorrelation is equal to the weight of the code (which is 5 in this example) and it occurs at a normalized delay of 1.

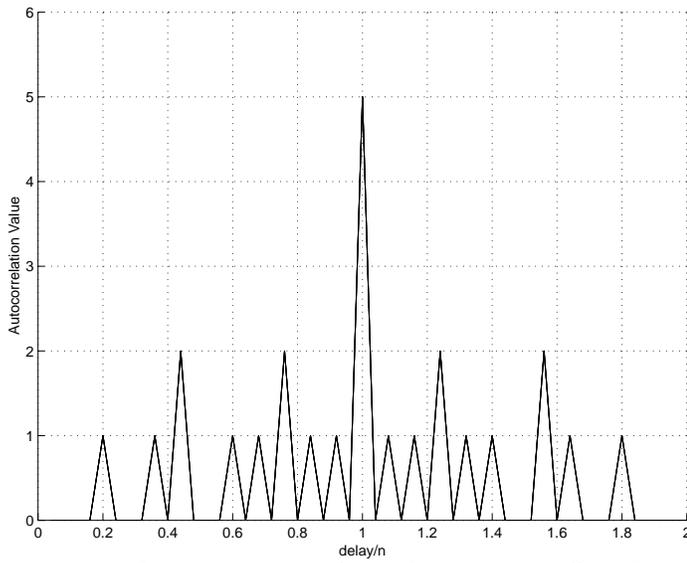


Figure 2: Autocorrelation of codeword  $C_1$  of a  $(25,5,2,2)$  OOC based on Quadratic Residues.

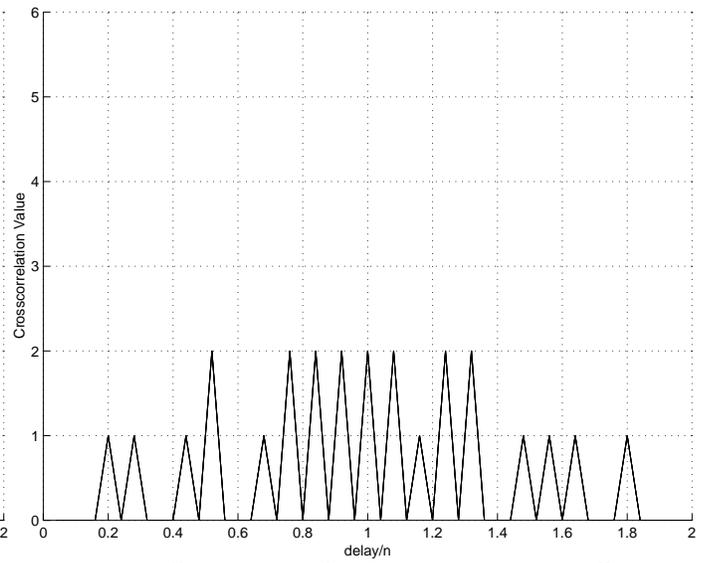


Figure 4: Crosscorrelation between codeword  $C_1$  and codeword  $C_3$  of a  $(25,5,2,2)$  OOC based on Quadratic Residues.

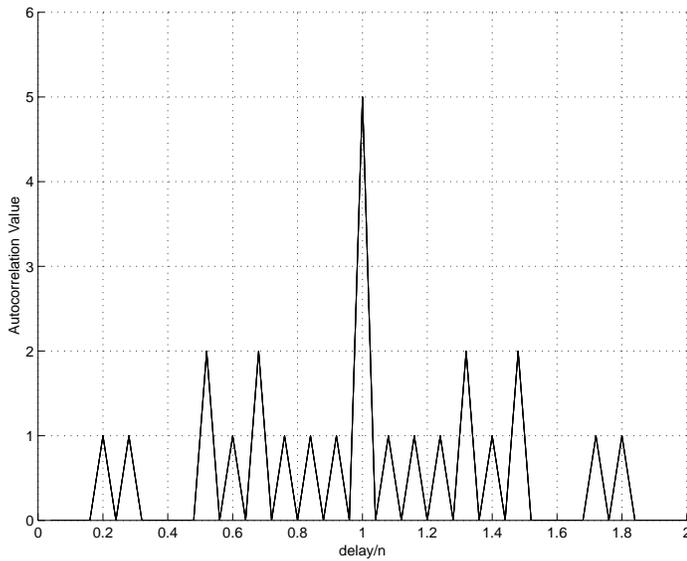


Figure 3: Autocorrelation of codeword  $C_3$  of a  $(25,5,2,2)$  OOC based on Quadratic Residues.

The maximum off-peak autocorrelation value (side-lobe) in all the plots never exceeds 2. The plots differ for different codewords because the distribution of 1's in them is different. The crosscorrelation between codewords  $C_1$  and  $C_3$  of example 3.1 is shown in Fig. 4. Fig. 5 shows the crosscorrelation between codewords  $C_2$  and  $C_4$ . As can be seen from Figs. 4 and 5, the maximum crosscorrelation value between any two codewords never exceeds 2.

### 3.2. Properties of OOCs using Quadratic Residues

The OOCs based on Quadratic Congruences have a very high maximum value of crosscorrelation between any two codewords,  $\lambda_c = 4$ , and the maximum off-peak autocorrelation value,  $\lambda_a = 2$ . The OOCs proposed in this paper using Quadratic Residues have a maximum value of crosscorrelation between any two codewords,  $\lambda_c = 2$  while having all other code parameters the same as that in Quadratic Congruence codes.

Therefore the OOC is of the form  $(p^2, p, 2, 2)$ .

The codewords of example 3.1 have the following properties:

- The length of the codeword,  $n = p^2 = 25$
- The weight of the codeword,  $w = p = 5$
- The maximum value of off-peak autocorrelation,  $\lambda_a = 2$
- The maximum value of crosscorrelation,  $\lambda_c = 2$
- The number of codewords,  $M = p - 1 = 4$

## REFERENCES

- [1] J. A. Salehi, "Code Division Multiple-Access Techniques in Optical Fiber Networks - Part I : Fundamental Principles," IEEE Trans. on Communications, vol. 37, no. 8, pp. 824-833, August 1989.
- [2] J. A. Salehi and C. A. Brackett, "Code Division Multiple-Access Techniques in Optical Fiber Networks - Part II : Systems Performance Analysis," IEEE Trans. on Communications, vol. 37, no. 8, pp. 834-842, August 1989.
- [3] A. A. Shaar and P. A. Davis, "Prime Sequences : Quasi-Optimal Sequences for OR Channel Code Division Multiplexing," Electronic Letters, vol. 19, no. 21, pp. 888-889, October 1983.
- [4] S. V. Marić, Z. I. Kostić and E. L. Titlebaum, "A New Family of Optical Code Sequences for Use in Spread-Spectrum Fiber-Optic Local Area Networks," IEEE Trans. on Communications, vol. 41, no. 8, pp. 1217-1221, August 1993.
- [5] F. R. K. Chung, J. A. Salehi and V. K. Kei, "Optical Orthogonal Codes : Design, Analysis and Applications," IEEE Trans. Information Theory, vol. 35, no. 3, pp. 595-604, May 1989.
- [6] Manoj Choudhary, P. K. Chatterjee and Joseph John, "Code Sequences for Fiber Optic CDMA Systems," Proc. of National Conference on Communications 1995, IIT Kanpur, pp. 35-42, 1995.
- [7] Manoj Choudhary, P. K. Chatterjee and Joseph John, "Optical Orthogonal Codes using Hadamard Matrices," Proc. of National Conference on Communications 2001, IIT Kanpur, pp. 209-211, 2001.
- [8] Manoj Choudhary, P. K. Chatterjee and Joseph John, "Optical Orthogonal Codes using Error Correcting Codes," Proc. of National Conference on Communications 2002, IIT Mumbai, pp. 65-69, 2002.
- [9] Manoj Choudhary, "Studies on Some New Classes of Optical Orthogonal Codes," Ph.D Thesis, IIT Kanpur, August 2001.

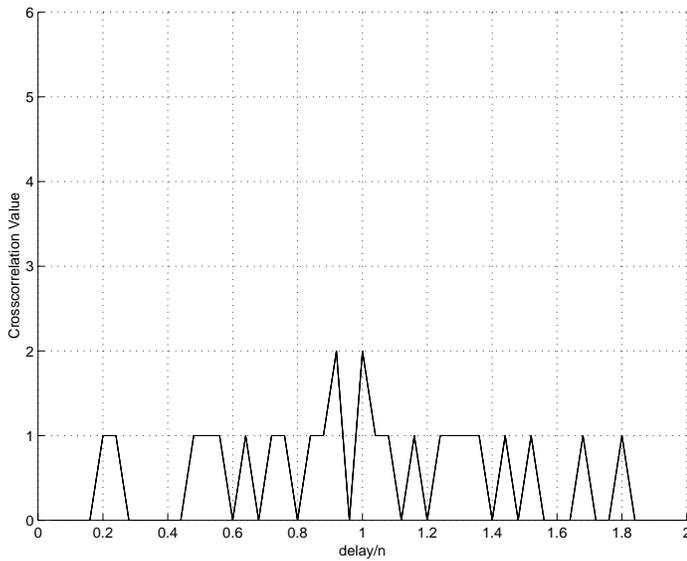


Figure 5: Crosscorrelation between codeword  $C_2$  and codeword  $C_4$  of a  $(25,5,2,2)$  OOC based on Quadratic Residues.

The OOCs suggested in this paper have the same number of codewords in them as that of the OOCs obtained using Quadratic Congruences. For the same number of codewords, these codes appear to be much more useful than the OOCs obtained using Quadratic Congruences because of the superior crosscorrelation parameters i.e., the value of  $\lambda_c$  is now only 2 instead of 4.

## 4. CONCLUSION

In this paper, we presented a method of constructing OOCs using the Quadratic Residues. These codes can be used in any optical CDMA application such as a FO-CDMA system. The OOCs are of form  $(p^2, p, 2, 2)$ , where  $p$  is a prime. We included one example to illustrate the construction method. We see that the codes presented in this paper have better crosscorrelation properties than the OOCs obtained using Quadratic Congruences, while keeping all the other code parameters exactly the same.